

OCTO Privacy Policy

Version 1.4.4 · Updated 6 October 2026 · English

Current review — registration and subscriber emails remain paused.

This version reflects the live website and the selected limited security/delivery approach. Remaining email-tracking, provider and retention checks must be resolved before registration and subscriber sending resume. The notice does not certify that an exemption applies.

1 Who we are and what this policy covers

Axel Van Mechelen and Robbe Heynderickx operate OCTO in their own names and are joint data controllers. OCTO is currently a project, with no registered business or VAT number. Contact either founder through admin@octo-tool.com, +32 472 97 43 23, or Isabellakaai 60, 9000 Ghent, Belgium.

Axel coordinates privacy information and requests. Robbe coordinates suppliers, security, deletion and backup expiry. Both remain responsible for the joint processing; you may exercise your rights against either founder. This is the essence of our allocation of responsibilities; ask us for further information about the arrangement.

This policy covers our public website, contact with us, and the free waitlist and optional newsletter when available. New registrations and subscriber emails are currently paused. We will provide separate privacy information before offering product accounts, uploads, AI chats or payments.

2 Website, cookies and browser storage

We receive information from your browser, your messages and submissions, and service providers' security and email-delivery records. Website requests can include your IP address, browser and device details, requested pages and error records. We use necessary technical data to deliver and protect the website, on the basis of legitimate interests in operating a secure service (Article 6(1)(f) GDPR). Our retention rule for OCTO-controlled routine technical and delivery logs is up to 30 days; section 6 explains the outstanding verification of provider logs.

Cookiebot by Usercentrics remembers your cookie choice. Managing and recording consent supports our consent obligations (Article 6(1)(c)). The language preference provides the setting you request (Article 6(1)(f)). Optional Google Analytics 4 (GA4) requires separate consent (Article 6(1)(a)). Merely browsing, joining the waitlist or accepting the Terms does not grant analytics consent.

Current browser storage, checked on 6 October 2026

Name and provider	Purpose and scope	Lifetime and choice
CookieConsent — Cookiebot / Usercentrics	Consent identifier, time and category choices. First-party cookie on the visited OCTO hostname, path /.	One calendar month after your choice. Necessary to remember and apply that choice; a new choice may reset its expiry.
_ga — Google	Pseudonymous browser identifier. Cookie on octo-tool.com (including subdomains), path /.	Up to 180 days from setting. Its expiry did not renew in our revisit check. Statistics consent required.
_ga_CCXN1DEMRF — Google	Analytics session information. Cookie on octo-tool.com (including subdomains), path /.	Up to 180 days; activity can renew this session cookie's expiry. Statistics consent required.
octo-language — OCTO	Local storage on each website origin, containing the language you explicitly select (English or Dutch). It is not an analytics cookie.	No automatic expiry. Remove it through Cookie settings or your browser's site-data controls.

Cookiebot also holds consent records separately from the browser cookie. Its [published policy](#) states a 12-month retention period for End User Data. This is distinct from OCTO's one-month browser-choice setting; the account-specific record and deletion arrangements remain under review.

Cloudflare Turnstile is configured to check new waitlist and newsletter signups for automated abuse using browser, device and network signals. Pre-clearance is disabled; it is not required to unsubscribe. The full security-storage inventory for the paused signup flow still needs verification before reopening. We do not represent this table as a verified inventory of every provider-internal security record. See [Cloudflare's Turnstile notice](#).

3 Optional analytics

GA4 is available on the public website but loads only after you allow statistics cookies. Rejecting them leaves the website available. Our controls block Google Analytics requests, including cookieless signals, before consent and after rejection or withdrawal. Analytics does not load on confirmation, newsletter or email-preferences pages.

With consent, we measure visits and sessions, page views, 90% scrolling, waitlist-button clicks, form starts, accepted signup requests and language changes. An accepted request is not proof of a confirmed subscriber. Data include pseudonymous browser/session identifiers, timestamps, fixed page names, referring-site origins, approved campaign labels, browser/device details, language and approximate location. We do not send email addresses, optional answers, signed links or other form content to GA4, or link analytics to waitlist records. Advertising features, Google signals and user-provided data collection are disabled.

Google describes IP addresses as used to derive location without storing them in GA4. Analytics data are pseudonymous, not anonymous. User and event retention is configured to two months without resetting on new activity, subject to Google's deletion cycle. This setting does not govern browser-cookie expiry or aggregated standard reports. We review the need for those reports annually and delete the property when the website-improvement purpose ends.

Use [Cookie settings](#) at any time to change or withdraw your choice. Withdrawal stops further measurement, removes the GA cookies we control and reloads a page that loaded Analytics; this can reset an unfinished form. It does not automatically erase past measurements. You may request deletion

and, where needed, supply a browser identifier so we can locate the relevant data. Your choice is browser-specific; changing device, clearing storage or expiry may require a new choice.

4 Waitlist, newsletter and contact data

4.1 Free waitlist and optional answers

When registration is available, we use your email address, selected language, request/confirmation times and participation status to process your request, verify your address and send the availability notification you request, with your consent (Article 6(1)(a)). The email address and required declarations are necessary to apply; providing them is voluntary. We do not ask for your name or date of birth.

We record your age-group declaration (16–17 or 18+), parental/guardian-permission declaration where required, Terms acceptance, and consent choices with their timestamps, versions, displayed wording and relevant document reference/hash. The 16+ eligibility rule and permission requirement for 16–17-year-olds are OCTO participation rules, not a statement of the general GDPR consent age. We do not require an identity document as part of ordinary registration.

Education level and how you found us are optional, with separate purpose-specific choices. We use education to plan introductory groups and referral answers to improve communication. You may skip either question or withdraw permission for an answer separately. These purposes rely on consent (Article 6(1)(a)).

A submitted request is pending until you confirm your email. The waitlist verification link expires after 48 hours. Our deletion rule for an unconfirmed request is within 30 days after link expiry. For confirmed participation, the active-profile rule is until withdrawal, launch/closure of the waitlist or the end of 31 January 2027 in Brussels, whichever comes first, followed by deletion or irreversible anonymisation within 30 days. Continuing afterwards requires a new choice. Separate valid newsletter consent is handled independently. These are the operating limits to be verified before registration resumes, as explained in section 6.

4.2 Optional newsletter and email delivery

Newsletter marketing needs separate consent and separate confirmation (Article 6(1)(a)); joining the waitlist does not subscribe you. We process your email, language, newsletter status, preferences and consent evidence. Unconfirmed newsletter links expire after 14 days; the deletion rule is within 30 days afterwards. Confirmed marketing ends on withdrawal, the end of the activity or 24 months after the last explicit confirmation, whichever is earlier. Sending must stop when permission ends; the active marketing profile must be removed within 30 days, subject to the separate evidence and suppression rules below.

Security and delivery are our only intended uses of email technical records. Brevo processes recipient addresses, message content, delivery status, bounces, complaints and related technical records. OCTO uses the records needed to deliver requested messages, protect verification and recovery, investigate misuse and honour opt-outs. Our waitlist system does not import open/click events for engagement analytics. We do not use email-open or click histories for marketing profiles, personalised promotions, scoring or behaviour-triggered marketing.

Ordinary delivery and security processing relies on our legitimate interests in providing and protecting requested communications (Article 6(1)(f) GDPR), subject to necessity, proportionality and your rights. This basis does not itself permit access to information on your device. Any use of an email tracker without consent must separately satisfy the applicable strictly necessary transmission or requested-service exemption. We do not treat a provider's general reference to security, anti-abuse or deliverability as proof that every pixel, redirect or event history qualifies. Optional engagement measurement would require a separate lawful arrangement and, where required, prior valid consent before it starts.

What Brevo currently does. Brevo can insert an invisible image and rewrite links through its servers. Opening a message or following a rewritten link may create event times and counts linked to the message or recipient. Both account-wide anonymous-tracking settings are enabled and OCTO sets the available per-contact tracking preference to No. Those settings do not remove the pixel or link rewriting. Our latest controlled checks found anonymised main logs but open/click counts and times still visible within the recipient's message details. We therefore do not promise tracking-free messages or complete unlinking from individuals.

Subscriber sending remains paused. Before reopening, we must establish which residual operations are necessary for the stated security or delivery purpose, the minimum data and retention required, provider responsibilities and the applicable legal conditions. Operations outside a substantiated exemption must be disabled or handled through effective consent controls. Merely joining the waitlist, requesting a newsletter, accepting the Terms or allowing website analytics does not grant permission for unrelated email tracking. A revised notice does not retrospectively authorise earlier processing.

You can object to processing based on legitimate interests or make a privacy request at admin@octo-tool.com. We assess such requests under the applicable GDPR rules, including the unconditional right to object to direct marketing. Newsletter unsubscribe and leaving the waitlist stop the corresponding sending permission; they do not remove pixels from messages already received. Requests concerning those messages and Brevo's existing records require provider handling. We cannot promise that changing a preference deletes every provider log or backup; section 6 distinguishes our retention rules from provider periods.

4.3 Enquiries and essential notices

We use your contact details and message to answer enquiries on the basis of legitimate interests (Article 6(1)(f)), or Article 6(1)(b) for pre-contract steps you request. Our rule is to retain correspondence for up to 12 months after resolution, apart from a specific legal obligation or dispute. Neo supplies our mailboxes.

The same enquiry rules cover investor and pitch-deck requests, mentoring, student collaboration, technical introductions, press and ocean-initiative enquiries. Relevant correspondence may include your name, organisation, contact details, interests and attachments that you choose to send. These pages open your own email application; submitting an enquiry does not subscribe you to marketing or create an investment, employment or collaboration agreement. Please do not send unnecessary sensitive information or third-party personal data without an appropriate reason.

Our social-media and research links take you to external services when you choose to follow them. Those services apply their own privacy information. We do not load social-media tracking embeds simply because you view an OCTO page. Data in correspondence are handled through our mailboxes, separately from waitlist and analytics records.

Necessary participation, closure or material-Terms notices serve administration of the waitlist agreement (Article 6(1)(b)); security and misuse notices serve legitimate interests (Article 6(1)(f)), or a legal obligation where applicable (Article 6(1)(c)). They must contain no promotional material and do not require newsletter consent. We keep only the contact and delivery evidence needed for the relevant purpose and period. The sending pause does not remove our duty to answer privacy requests or provide legally required notices.

5 Providers, sharing and international transfers

We do not sell personal data. The following providers support the service. Public provider terms explain possible processing arrangements; they are not proof that every account-specific contract, location or safeguard has been checked.

- **Cloudflare:** Pages hosting and network security process website requests; Turnstile checks signup abuse. R2 holds encrypted OCTO backups in an EU-jurisdiction bucket. That bucket restriction does not establish that all Cloudflare support, network or security processing stays in the EEA. [Cloudflare data processing terms](#).
- **Supabase:** forms, database and server functions handle submitted data, participation, consent/Terms evidence and delivery jobs. The current project region is eu-west-1 (Ireland). This does not restrict every support or subprocessor operation to Ireland. [Supabase data processing terms](#). Its account documents confirm that the data processing addendum is incorporated into the Terms for all organisations.
- **Brevo:** requested emails and optional newsletter delivery use addresses, preferences, content, delivery records and the tracking operations described in section 4.2. Its public hosting information identifies France and Germany; other processing, support and subprocessors require separate checks. [Brevo hosting information](#).
- **Neo:** hosts our contact mailboxes and handles correspondents' addresses, messages, attachments and mailbox records. Our account's processing locations, retention and transfer arrangements are still being verified. [Neo privacy information](#).
- **Cookiebot / Usercentrics A/S, Denmark:** supplies the consent interface, technical delivery and consent records. Its one-month browser choice and published 12-month End User Data period are distinct. Account-specific locations, subprocessors and contractual coverage remain to be checked. [Cookiebot privacy information](#).
- **Google Ireland Limited, with Google LLC and authorised subprocessors:** supplies optional GA4 and receives the analytics data in section 3. Processing may occur in the United States and other countries. [Google processing terms](#) and [transfer arrangements](#).

Providers may process data outside the European Economic Area. Such transfers require an applicable adequacy decision or appropriate safeguards, such as Standard Contractual Clauses with the necessary assessment and supplementary measures. The EU–US Data Privacy Framework can apply only to an eligible transfer to an actively certified recipient. Cookie consent does not substitute for transfer safeguards.

Verification outstanding: we have not completed the provider-by-provider record of contracting entities, accepted processing agreements, all locations/subprocessors, applicable transfer mechanisms and deletion terms. The public links above do not resolve that gap. Contact us for the information currently available or a copy of applicable safeguards. We will update this notice as the verification is completed.

We may disclose necessary information to professional advisers or competent authorities where required for a legal obligation or justified claim. Access must be limited to the task, with confidentiality and processing terms where required.

6 Retention, deletion and security

Axel handles privacy requests; Robbe owns the manual deletion and backup-expiry process. Automated permanent cleanup is not enabled. The periods above and below are our documented operating rules, not evidence that every historical record or provider copy has already been deleted. Provider log lifetimes, mailbox cleanup and backup expiry have not yet been fully verified. Registration and subscriber email sending remain paused pending those checks.

Limited consent and privacy-request evidence supports legal obligations (Article 6(1)(c)); necessary Terms, eligibility and claim evidence supports legitimate interests in administering and defending the arrangement (Article 6(1)(f)). Keep only necessary evidence, normally for up to three years after

participation/consent ends or a request is resolved. A longer period requires a specific legal requirement or claim, with a recorded review date.

Minimal suppression records prevent unwanted re-import or sending while that risk exists and are reviewed annually. They do not permit continued marketing. The rule for OCTO-controlled backup copies is a maximum of 90 days from their original creation, with deletion requests reapplied before any restored data are used. Copying a backup must not restart its lifetime. Provider-internal copies have separate contractual limits that still need confirmation; we cannot describe them as covered by OCTO's backup rule.

We use encrypted connections and restricted access; no security measure guarantees absolute protection. We do not make solely automated decisions with legal or similarly significant effects or create behavioural advertising profiles. When consent ends, identifiable data must be erased without undue delay unless another valid basis permits limited retention. Truly anonymous statistics may be kept longer.

Google's processing terms describe up to 180 days for certain service-supported deletion instructions or end-of-term deletion, subject to their conditions. This is not a general OCTO retention period and does not extend the GDPR deadline for responding to your request.

7 Your rights and separate choices

Subject to GDPR conditions, you can request access, correction, erasure, restriction and portability; object to legitimate-interest processing for reasons relating to your situation; and object to direct marketing at any time. You may withdraw consent without affecting earlier lawful processing.

[Cookie settings](#) controls analytics. Newsletter unsubscribe controls marketing. [Email preferences](#) separates waitlist participation, newsletter permission and optional answers. Leaving one purpose does not automatically end another valid purpose. Stopping emails or removing an optional answer is not the same as erasing all records across the database, mailboxes, providers and backups.

For full erasure or another privacy request, contact admin@octo-tool.com or either founder at our postal address. We will explain any data that must be retained and the reason. We respond without undue delay and within one month. A permitted extension of up to two further months requires an explanation within the first month. Requests are normally free; if we reasonably doubt identity, we ask only for what is necessary to verify it.

Preference changes are saved in OCTO first; updates to Brevo are queued and may take time. A message already accepted by the email provider for delivery may still arrive. We check current permission before further sending and investigate failed synchronization; a delay does not restore consent.

8 Complaints and changes

You may complain directly to the [Belgian Data Protection Authority](#) or another competent EEA supervisory authority and seek a judicial remedy. You do not have to contact us first.

We date revisions, preserve previous versions and notify affected people of material changes where required. A new purpose requires fresh consent where applicable. This release is available in English and Dutch.